

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] A file memory means to memorize the multiple files enciphered using two or more encryption algorithms, A description storage means to match and memorize an operator's body information and decryption algorithm, A decryption algorithm specification means to search said description storage means and to specify a decryption algorithm based on an operator's body information that it was inputted from the exterior, A processing means to decode the file memorized by said file memory means with the decryption algorithm specified by said decryption algorithm specification means, and to access it, The computer system characterized by making accessible only the file which can be decoded with the decryption algorithm specified using a preparation and body information.

[Claim 2] A file memory means to memorize the multiple files enciphered using two or more encryption algorithms, An access-permission condition storage means to match and memorize an operator's body information that access of the file memorized by said file memory means and this file is accepted, A detection means to detect the demand of access to the file memorized by said file memory means, A means to require the input of an operator's body information when said detection means detects said demand, An access-permission distinction means to distinguish whether access to the file memorized by said file memory means based on the physical information inputted from the exterior is accepted with reference to said access-permission condition storage means, When access was permitted and said access-permission distinction means distinguishes The computer system characterized by having the access means which makes said file accessible by loading the program for performing the algorithm which decodes this file, and performing this program.

[Claim 3] It is the computer system according to claim 1 or 2 characterized by what said encryption algorithm is an algorithm compressed while enciphering data, and said decryption algorithm consists of an algorithm elongated while decrypting the enciphered data.

[Claim 4] The computer system according to claim 1, 2, or 3 characterized by what a means to display the message which stimulates the input of the body information by body information reading means to read said operator's body information, and said body information reading means is included for.

[Claim 5] It is the computer system according to claim 4 which said body information consists of fingerprint data, data of a retina pattern, data of a voice pattern, or data of a face image, and is characterized by what said body information reading means consists of a fingerprint reader, a retina pattern reader, a voice pattern reader, or a face image reader for.

[Translation done.]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention relates to the computer system which distinguishes whether it has the authority to perform each processing from body information, such as a fingerprint, about the security technique of a computer.

[0002]

[Description of the Prior Art] When the user name and password which registered the user (operator) name and the password into the computer beforehand, were made to enter a user name and a password at the time of a log on etc. for the security of a computer, and were entered are not registered into a computer system, the method of not accepting a log on is learned.

[0003]

[Problem(s) to be Solved by the Invention] However, a burden is placed on a user in security with a user name, a password, etc., such as setting up a password or changing a password periodically so that others cannot presume easily. Moreover, when user ID etc. was set up by the system administrator, the burden of memorizing and making a note of user ID was placed. Furthermore, whenever there was a demand from a computer system, a user name, a password, user ID, etc. had to be inputted from the keyboard etc., and actuation was complicated.

[0004] since [moreover,] a note of the user ID and the password which were given [whether activation is permitted and or not] by the approach of checking by user ID is made, or there is the need for memorizing etc., a user **** during a session and the others may take a seat by every place in a session -- security -- taking all possible measures -- having been hard .

[0005]. This invention was not made in view of the above-mentioned actual condition, and aims at offering the computer system which does not apply the burden of security to a user.

[0006]

[Means for Solving the Problem] In order to attain the above-mentioned object, the computer system concerning the 1st invention A file memory means to memorize the multiple files enciphered using two or more encryption algorithms, A description storage means to match and memorize an operator's body information and decryption algorithm, A decryption algorithm specification means to search said description storage means and to specify a decryption algorithm based on an operator's body information that it was inputted from the exterior, A processing means to decode the file memorized by said file memory means with the decryption algorithm specified by said decryption algorithm specification means, and to access it, It is characterized by making accessible only the file which can be decoded with the decryption algorithm specified using a preparation and body information.

[0007] In order to attain the above-mentioned object, the computer system concerning the 2nd invention A file memory means to memorize the multiple files enciphered using two or more encryption algorithms, An access-permission condition storage means to match and memorize an operator's body information that access of the file memorized by said file memory means and this file is accepted, A detection means to detect the demand of access to the file memorized by said file memory means, A means to require the input of an operator's body information when said

detection means detects said demand, An access-permission distinction means to distinguish whether access to the file memorized by said file memory means based on the physical information inputted from the exterior is accepted with reference to said access-permission condition storage means, When access was permitted and said access-permission distinction means distinguishes The program for performing the algorithm which decodes this file is loaded, and it is characterized by having the access means which makes said file accessible by performing this program.

[0008] According to these configurations, a decryption algorithm is specified based on an operator's body information. Therefore, each operator can access only the file which can be decoded using this decryption algorithm, and cannot access other files. Therefore, only those who have just authority can access each file. Moreover, it is not necessary to enter a user name, a password, etc. one by one, and operability is also high.

[0009] Said encryption algorithm is an algorithm compressed while enciphering data, and, as for said decryption algorithm, what is consisted of an algorithm elongated while decrypting the enciphered data is desirable. Such a configuration, then the limited file memory means of capacity can be used effectively.

[0010] A means to display the message which stimulates the input of the body information by body information reading means to read said operator's body information, and said body information reading means may be established.

[0011] Said body information consists of fingerprint data, the data of a retina pattern, data of a voice pattern, data of a face image, etc. In this case, said body information reading means consists of a fingerprint reader, a retina pattern reader, a voice pattern reader, a face image reader, etc.

[0012]

[Embodiment of the Invention] Hereafter, the gestalt of implementation of this invention is explained with reference to a drawing.

(Gestalt of the 1st operation) With reference to drawing 1 - drawing 4 , the computer system concerning the gestalt of implementation of the 1st of this invention is explained.

[0013] As shown in drawing 1 , this computer system consists of buses B which connect these with a fingerprint reader 1, a keyboard 2, an indicating equipment 3, external storage 4, memory 5, and a control section 6.

[0014] A fingerprint reader 1 reads the image of human being's fingerprint, and supplies the image data to the body 1 of a computer through a RS232C interface etc.

[0015] A keyboard 2 is an input unit for inputting data, such as an alphabetic character, a notation, and a figure. An indicating equipment 3 consists of CRT, a liquid crystal display, etc., and displays the message to the data inputted from the keyboard 2, and an operator etc.

[0016] External storage 4 consists of hard disk drive units etc., and where the file (a program, a text file, an image file, etc. are included) which a control section 6 processes is enciphered, it is memorized. For example, when using this computer system by three persons, A, B, and C, as shown in drawing 2 , the file which A accesses is enciphered by encryption algorithm Ha, the file which B accesses is enciphered by encryption algorithm Hb, and the file which C accesses is enciphered by encryption algorithm Hc. External storage 4 memorizes a control program 11 and a user master file. A user master file is the fingerprint data of A, B, and C, encryption program PHa-PHc, and decryption program PHa-1-PHc-1. It matches and memorizes. A control program 11 controls encryption and a decryption program. The control program 11 is set up so that it may start following starting of OS (operating system).

[0017] Memory 5 consists of RAM (Random Access Memory) etc., and functions as main memory, a work area, etc. of a control section 6. A control section 6 consists of MPU (Micro Processing Unit) etc., performs the program stored in main memory, and directs writing or reading of fingerprint reading, image display, and data to a fingerprint reader 1, an indicating equipment 3, and external storage 4, respectively. Moreover, a control section 6 performs processings, such as processing of data, such as an alphabetic character inputted from processing of the image data of the fingerprint

read by the fingerprint reader 1 and a keyboard 2, processing of the screen data displayed on an indicating equipment 3, reading processing of the data from external storage 4, and writing of the data to external storage 4.

[0018] Next, actuation of the computer system of the gestalt of this operation is explained with reference to the flow chart of drawing 3. If this computer system is started, first, OS will be started (S11), then a control program 11 will be started (S12).

[0019] Next, a control program 11 displays the message of a purport which should input a fingerprint on a display 3 (S13). Furthermore, reading of a fingerprint is directed to a fingerprint reader 1 (S14). An operator inputs a fingerprint from a fingerprint reader 1 according to this display (S15). A fingerprint reader 1 stores the read image data (image data of a fingerprint) in memory 5 through an interface. A control program 11 codes the image data of the fingerprint stored in memory 5, and generates coding fingerprint data (S16). Next, coding fingerprint data and the fingerprint data of a user master file are collated (S17), and it distinguishes whether there is any match (S18).

[0020] When there is a match, it judges that it is admitted that that operator uses this computer system, and as shown in drawing 4, a control program 11 and encryption / decryption program corresponding to main memory (memory 5) are made resident (S19). The program data enciphered using the decryption program are decrypted at the time of data reading ****, and henceforth it reads, and a program is performed at the time of data writing ****, enciphering using an encryption program and writing in program data etc.

[0021] On the other hand, when the image data of the fingerprint read in the fingerprint reader 1 judges that it is in agreement with neither of the fingerprint data registered into the user master file (S18), a control program 11 judges that it is not admitted that that operator uses this computer system, and stops the resident of the control program 11 to main memory (S20). Henceforth, it shifts to the usual actuation.

[0022] According to such a configuration, encryption / decryption program corresponding to [utilization time / of those who are permitted the activity of a computer] an operator in a control program 11 resides in main memory permanently. Therefore, as shown in drawing 2, the various data stored in external storage 4 can be decoded by the decryption program, can be read as a usual program or data, and can be processed. Moreover, under control of a control program 11, an encryption program can be used, it can encipher, and the data created and processed can be stored in external storage 4.

[0023] And only encryption / decryption program corresponding to the operator specified by coding fingerprint data resides in main memory permanently. Therefore, each operator cannot access the file enciphered by the encryption algorithm for other operators. Therefore, access to each file can be limited to those who have just authority. On the other hand, when an operator is a non-registrant, a control program 11 does not reside in main memory permanently. Therefore, the program and the various data which are stored in external storage 4 cannot be restored. Therefore, it becomes difficult to use this system itself itself.

[0024] For example, when Operator A uses this computer system, A will be distinguished if the coding fingerprint data and the fingerprint data of A of a user master file which the fingerprint was inputted at step S15, and the image data of this fingerprint was coded at step S16, and were generated from the image data of the fingerprint of A at step S18 are in agreement. The encryption program PHa for A and its decryption program PHa-1 reside in main memory permanently with a control program 11 (S19).

[0025] Therefore, Operator A can access decrypting the programs 1 and 2 enciphered using the encryption program PHa, text files 1-3, an image file, etc. by decryption program PHa-1, can encipher further the document and image which were created and processed, and can store in external storage 4.

[0026] Here, even if A tends to access the file in which B has an access privilege, since the file of B is enciphered by the encryption program PHb, this cannot be decrypted by decryption program

PHa-1 which resides in main memory permanently. Therefore, A cannot access the file of B. Therefore, although external storage 4 is shared, a file can be used for the others in the state of secrecy.

[0027] (Gestalt of the 2nd operation) In the gestalt of the 1st operation, although fingerprint data were used for the personal authentication at the time of a log in, it is also possible to attest an operator for example, whenever access of a file is required. The gestalt of the 2nd operation which performs such processing is explained below.

[0028] The physical configuration of the computer system of the gestalt of this operation is the same as the configuration fundamentally shown in drawing 1. On the other hand, logically, the computer system of the gestalt of this operation consists of OS (operating system)21 and a file control program 31, as shown in drawing 5.

[0029] OS (operating system)21 is equipped with the input section 22 which detects the alter operation of a keyboard 2, the processing section 24 which performs processing according to the input directions detected by the input section 22, and the display and control section 23 which controls a display 3. The processing section 24 contains the file-processing section 25 for accessing a file.

[0030] On the other hand, the file control program 31 detects that the event occurred, and when the event is a thing about file manipulation, it is a program for or or controlling [to which the file manipulation is permitted] whether refusal is carried out.

[0031] It is an example when drawing 5 presupposes that OS21 is DOS (disk operating system), and the file control program 31 consists of the input hook section 32, the driver section 33, and a user master file 39.

[0032] When an interrupt request is published, the input hook section 32 does not make the processing which should be performed when the file control program 31 does not exist (when an event occurs) perform, but makes it process in the driver section 33 in advance of this processing (it hooks).

[0033] The user master file 39 consists of every user and a list of files which can be operated for every fingerprint data, as shown in drawing 6. In addition, this user master file 39 very thing is set up so that only the manager of this computer system can access. The driver section 33 consists of the content distinction section 34 of processing, the message indicator section 35, the coding section 36, the distinction section 37, and the transmitting section 38.

[0034] The content distinction section 34 of processing analyzes the input incorporated by the input hook section 32, and when it is being distinguished and directed whether the content is directing actuation of a file, it provides the distinction section 37 with input while it directs reading of a fingerprint in the coding section 36. Moreover, when the hooked input is not directing actuation of a file, a detecting signal is sent to the transmitting section 38.

[0035] The message indicator section 35 displays the screen to which the input of fingerprint information is urged on a display 3 through the display and control section 23 of OS21, when the content distinction section 34 of processing distinguishes saying "The input is directing actuation of a file." Moreover, when the distinction section 37 judges "the operator is not permitted the demanded file manipulation", the screen in which it is shown that access was refused is displayed on a display 3 through a display and control section 23.

[0036] The coding section 36 directs reading of a fingerprint to a fingerprint reader 1 according to the directions from the content distinction section 34 of processing, and captures the image of a fingerprint from a fingerprint reader 1, codes this, and generates coding fingerprint data.

[0037] The distinction section 37 distinguishes whether based on the coding fingerprint data generated in the coding section 36, those who have the coding fingerprint data have the authority to access an applicable file, with reference to the user master file 39. And when it is judged that it has authority, the signal with which access is permitted to the transmitting section 38 is transmitted. Moreover, when it did not have authority and distinguishes, the message of a purport which does not

permit access to the message indicator section 35 is displayed.

[0038] Actuation of the computer system of the gestalt of the 2nd operation is explained with reference to the flow chart of drawing 7 and drawing 8. First, the charge of the power source of a computer starts OS21 (S31). Next, the file control program 31 starts (S32). If the input hook section 32 of the file control program 31 starts, it will rewrite the address of the processing corresponding to the interrupt request which the input section 22 of OS21 generates to the address of the processing section 24 to the driver section 33. A paraphrase rewrites transmission places, such as a detecting signal of the key stroke which the input section 22 generates, to the address of the input hook section 32 (S33).

[0039] For example, in the case of MS-DOS (trademark) currently provided with OS21 from Microsoft Corp., let the address of the processing corresponding to the interrupt INT 21 of the system call about an input be the address of the driver section 33 among the interruption table created on the memory 5 which functions as main memory. Above, the setting-operation at the time of starting is ended.

[0040] In this condition, if there is a certain input from a keyboard 2, the input section 22 of OS21 will distinguish this alter operation, and will emit an interrupt request if needed (generating of IO event). Although processing corresponding to this interrupt request is usually performed in the processing section 24, it is rewritten by the address of the driver section 33 at the time of starting of the file control program 31. Therefore, processing shifts to the driver section 33 and is hooked (drawing 8, S41).

[0041] The content distinction section 34 of processing analyzes the detecting signal inputted from OS21 (S42), and distinguishes whether the content of an input is directing actuation (an execution file is started [opening a file,]) of a file (S43). When the content of an input is directing actuation of a file, reading of a fingerprint is directed to a fingerprint reader 1 through the coding section 36 (S44). Furthermore, the display of the message which urges the input of a fingerprint to the message indicator section 35 is directed (S45). The message indicator section 35 displays the message which urges the input of a fingerprint to an indicating equipment 3 through the display and control section 23 of OS21 according to directions of the content distinction section 34 of processing.

[0042] If the image entry of data of the fingerprint from a fingerprint reader 1 is stood by (S46) and image data is inputted, the coding section 36 will change this image data into coding fingerprint data, and will provide the distinction section 37 with it (S47). The distinction section 37 distinguishes whether actuation of a file in which those who have coding fingerprint data supplied from the coding section were directed by alter operation is accepted with reference to the user master file 39 (S48).

[0043] If the distinction section 37 judges that access is accepted, it will make an encryption program required in order to access the file at main memory, and a decryption program resident (S49). Then, the distinction section 37 supplies a detecting signal to the transmitting section 38. The transmitting section 38 hands over processing in the processing section 24 of OS21 (S50).

[0044] Henceforth, the processing section 24 decrypts and reads the file directed by the decryption program, enciphers by the encryption program and writes in the data processed and generated. If access of the file is completed, the file control program 31 will delete the compression program and decryption program on main memory.

[0045] On the other hand, when it is judged at step S48 that file manipulation is not accepted by the distinction section 37, the message indicator section 35 displays the message which refuses the file manipulation of "access is not permitted" to an indicating equipment 3 through the display and control section 23 of OS21 (S51). When the content distinction section 34 of processing judges that the content of directions is not actuation of a file at step S43, processing is handed over by the processing section 24 of OS21 by the transmitting section 38 (S52). The processing section 24 performs processing corresponding to these directions.

[0046] Moreover, in case shut [a system], after rewriting the address of the processing

corresponding to the interrupt request which the input section 22 of OS21 generates to the usual address, it ends. According to such a configuration, when starting of the program of arbitration is directed on a desktop, it is distinguished according to the user master file 39 whether these directions are hooked in the input hook section 32, and access is permitted in the distinction section 37, only in authorization, corresponding encryption / decryption program is started and that file can be accessed, for example.

[0047] As explained above, in the file control program's 31 distinguishing whether it has the authority to incorporate input directions automatically and to access the directed file based on coding fingerprint data and having authority, according to the gestalt of this 2nd operation, it permits access of that file. Therefore, the security protection of a computer can be performed, without applying a burden to a user.

[0048] Moreover, file manipulation can be controlled only by installing the file control program 31, and it is not necessary to add correction to the existing OS, an application program, etc., and can be used as it is.

[0049] In addition, in the above explanation, although the file control program 31 rewrote the address of the processing corresponding to the interrupt request of the input section 22 at the time of starting, at the time of install of the file control program 31, the address of the processing corresponding to an interrupt request may be rewritten, and you may rewrite to the original address at the time of uninstallation.

[0050] As for the program which realizes encryption algorithm and it, what is compressed while enciphering data is desirable, and, as for the program which realizes said decryption algorithm and it, what is elongated while decrypting the enciphered data is desirable. According to such a configuration, the storage capacity of external storage 4 can be used effectively.

[0051] OS21 is not limited to DOS but the thing of arbitration can be used for it for the so-called window system, unix, etc. What is necessary is just to distinguish whether an operator has the authority to access a file, while detecting predetermined events, such as access to a file or a demand of interruption, and generating of a link, suitably and urging a fingerprint entry of data according to the property of each OS in using these OS's.

[0052] In addition, a fingerprint reader 1 and the body of a computer may be connected in a network etc.

[0053] Although coding fingerprint data were used with the gestalt of the above operation for personal authentication, the class of fingerprint data is arbitrary. For example, it is also possible to carry out the Fourier transform of the image data of a fingerprint, to extract the topology, and to use this as fingerprint data. In this case, for example, whenever [correlation / of the topology registered beforehand and the topology extracted from the image read with the fingerprint reader] etc. is measured, and when whenever [correlation] is more than fixed level, it is judged that two fingerprints are in agreement.

[0054] Although the fingerprint was used with the gestalt of the above operation for personal authentication, it is also possible to use the blood vessel pattern of a retina, a voice pattern, the image of a face, etc. as authentication information.

[0055] In addition, the computer of this invention cannot be based on the system of dedication, but can be realized using the usual fingerprint reader etc. and the usual computer system. For example, the computer system which performs above-mentioned processing can be constituted by installing this program from the media (a floppy disk, CD-ROM, etc.) which stored the program for performing above-mentioned actuation in the computer which connected the fingerprint reader.

[0056] Moreover, communication media (medium which holds a program temporarily and fluidly like a communication line, a communication network, and communication system) are sufficient as the medium for supplying a program to a computer. For example, this program may be put up for the notice plate (BBS) of a communication network, and this may be distributed through a network. And above-mentioned processing can be performed by starting this program and performing like other

application programs under control of OS.

[0057]

[Effect of the Invention] Secrecy can be held without almost applying a burden to a user based on a user's body information according to this invention, as explained above.

[Translation done.]

*** NOTICES ***

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the physical configuration of the computer system by the gestalt of operation of the 1st of this invention.

[Drawing 2] It is the conceptual diagram showing the configuration of external storage.

[Drawing 3] It is the flow chart which shows the control processing at the time of starting performed in the control section of drawing 1 .

[Drawing 4] It is drawing showing the situation of encryption / decryption program **** data processing.

[Drawing 5] It is the block diagram showing the physical configuration of the computer system by the gestalt of operation of the 2nd of this invention.

[Drawing 6] It is drawing having shown the example of a user master file.

[Drawing 7] It is the flow chart which shows the processing at the time of the startup of the computer system of the gestalt of the 2nd operation.

[Drawing 8] It is the flow chart which shows the processing at the time of the alter operation of the computer system of the gestalt of the 2nd operation.

[Description of Notations]

1 Fingerprint Reader

2 Keyboard

3 Display

4 External Storage

5 Memory

6 Control Section

11 Control Program

[Translation done.]

*** NOTICES ***

JPO and NCIP are not responsible for any

damages caused by the use of this translation.

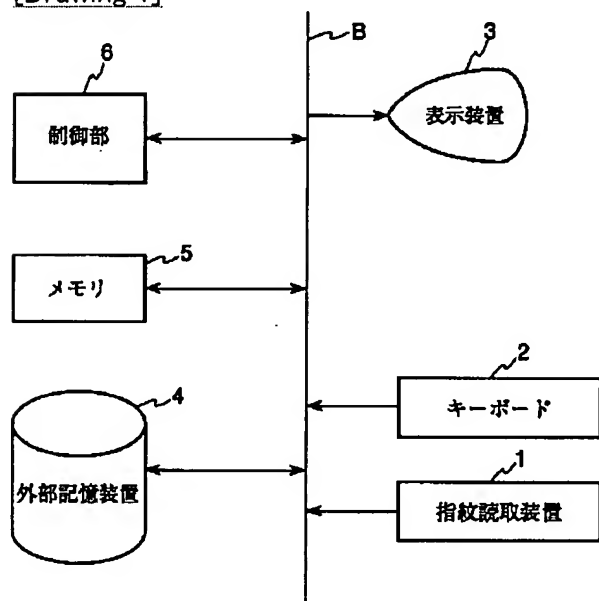
1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

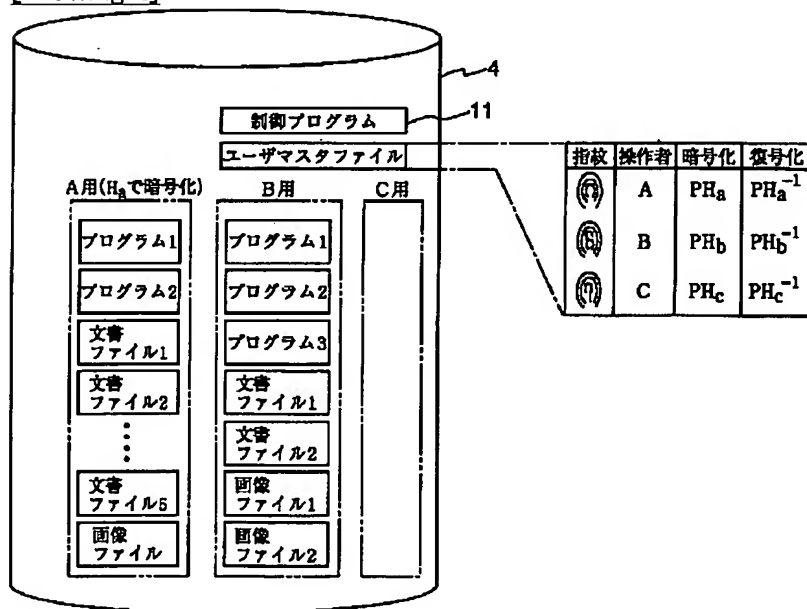
3.In the drawings, any words are not translated.

DRAWINGS

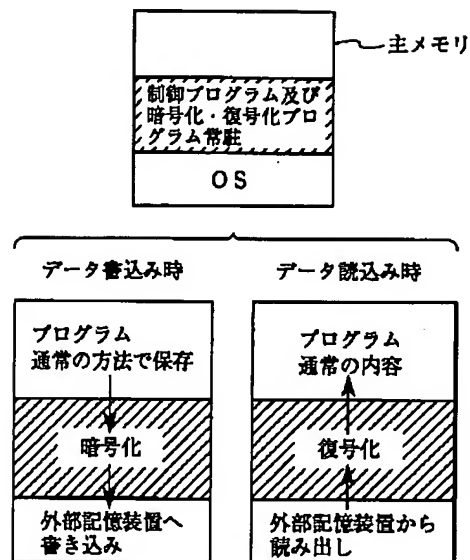
[Drawing 1]



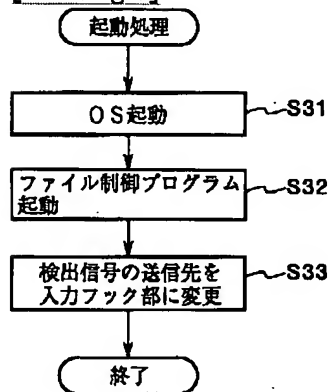
[Drawing 2]



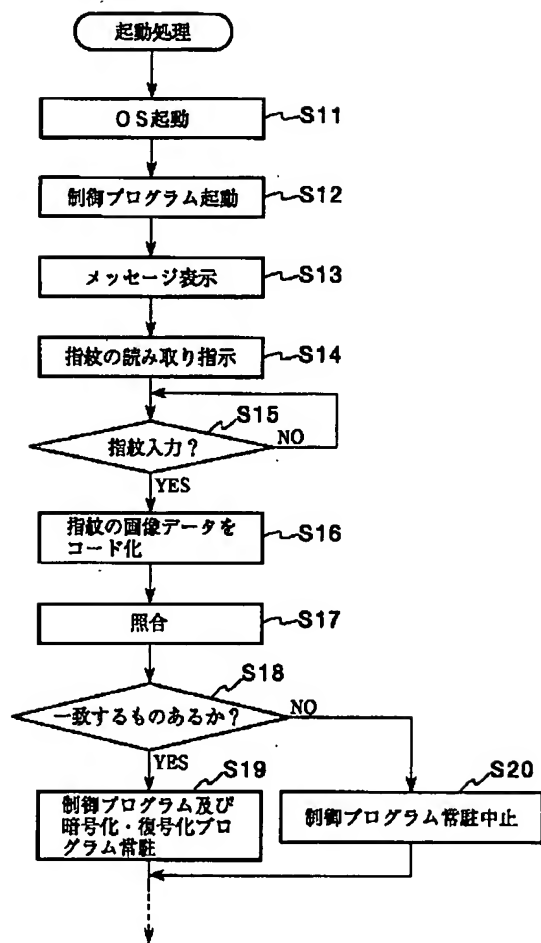
[Drawing 4]



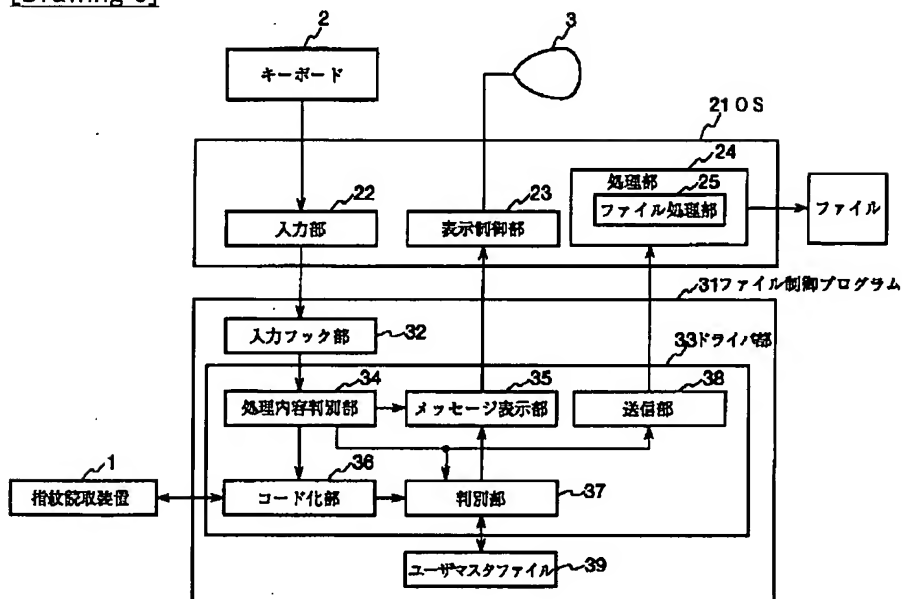
[Drawing 7]



[Drawing 3]



[Drawing 5]

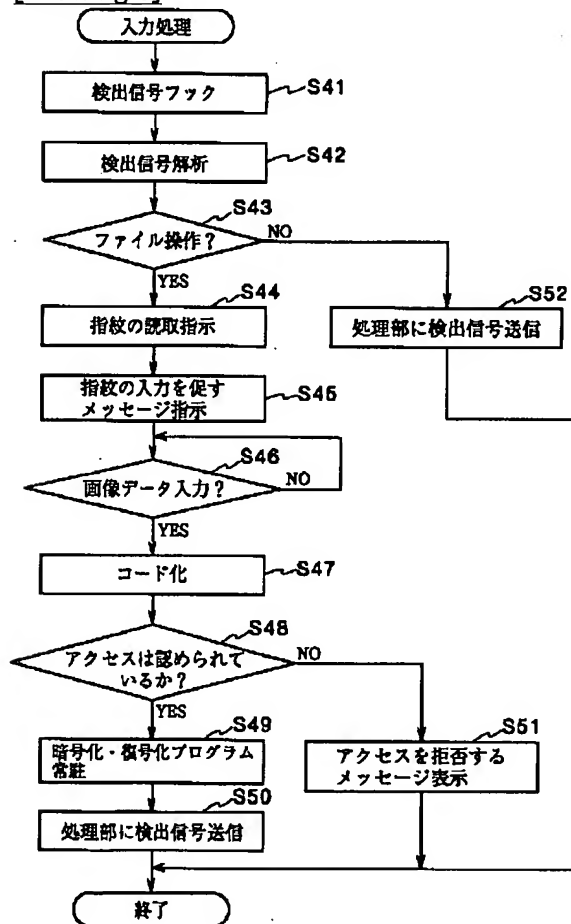


[Drawing 6]

	ファイル1	ファイル2	ファイル3	ユーザマスタ ファイル
A	○	○	×	×
B	×	○	○	×
...
Z	○	○	○	○

Z: システム管理者

[Drawing 8]



[Translation done.]

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-207777

(43)Date of publication of application : 07.08.1998

(51)Int.Cl.

G06F 12/14

G06F 12/00

H04L 9/32

(21)Application number : 09-008065

(71)Applicant : TSUBASA SYST KK

(22)Date of filing : 20.01.1997

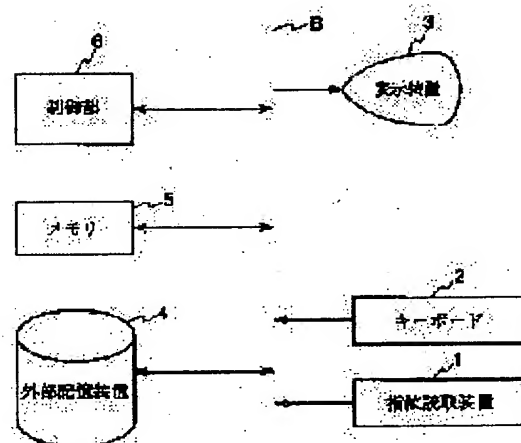
(72)Inventor : TSURUMURA YUKIZOU

(54) COMPUTER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a computer system in which security can be improved without forcing the load of attention to a user.

SOLUTION: An encipherment algorithm is decided for each operator, and a file for storing a file to which access is permitted to each operator is enciphered and stored in an outside storage device 4. At the time of activation, the picture of the fingerprint of the operator is read by a fingerprint reading device 1. A control part 6 specifies the operator from the picture of the fingerprint of the user, and allows corresponding encipherment and decipherment programs to be resident in a main memory. Afterwards, it is possible to perform access to the file which can be deciphered by the resident decipherment program. The files of others are enciphered by different encipherment algorithms so that access can be inhibited.



LEGAL STATUS

[Date of request for examination]

10.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-207777

(43) 公開日 平成10年(1998) 8月7日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 B

12/00

5 3 7

12/00

5 3 7 H

H 0 4 L 9/32

H 0 4 L 9/00

6 7 3 D

審査請求 未請求 請求項の数 5 O L (全 9 頁)

(21) 出願番号

特願平9-8065

(22) 出願日

平成9年(1997) 1月20日

(71) 出願人 594057314

翼システム株式会社

東京都江東区亀戸2丁目25番14号

(72) 発明者 鶴村 亨三

東京都江東区亀戸2丁目25番地14号 翼システム株式会社内

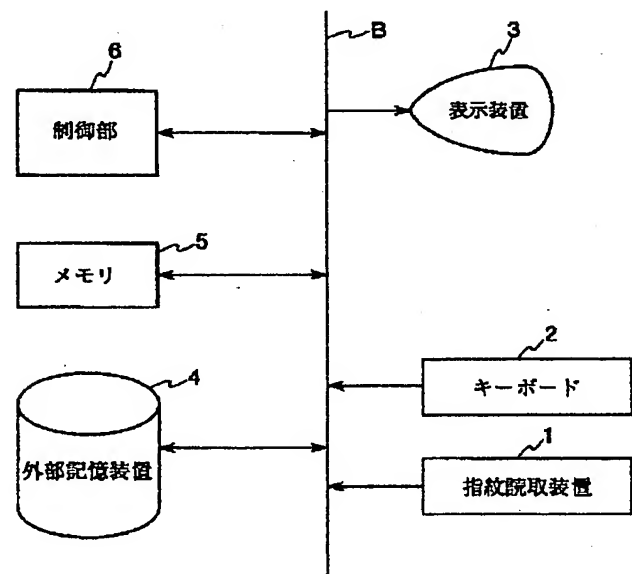
(74) 代理人 弁理士 木村 満 (外3名)

(54) 【発明の名称】 コンピュータシステム

(57) 【要約】

【課題】 ユーザに注意負担を強いることなく、セキュリティを高めることができるコンピュータシステムを提供する。

【解決手段】 外部記憶装置4に、操作者毎に暗号化アルゴリズムを定め、各操作者にアクセスが認められているファイルを格納するファイルを暗号化して格納する。起動時に、指紋読取装置1によって、操作者の指紋の画像が読み取られる。制御部6は、ユーザの指紋の画像から、操作者を特定し、対応する暗号化及び復号化プログラムを主メモリに常駐させる。以後、常駐している復号化プログラムで復号化できるファイルをアクセスできる。他者のファイルは、異なる暗号化アルゴリズムで暗号化されているため、アクセスすることはできない。



【特許請求の範囲】

【請求項1】複数の暗号化アルゴリズムを用いて暗号化された複数のファイルを記憶するファイル記憶手段と、操作者の身体情報と復号化アルゴリズムを対応付けて記憶する特徴記憶手段と、

外部より入力された操作者の身体情報に基づいて、前記特徴記憶手段を検索し、復号化アルゴリズムを特定する復号化アルゴリズム特定手段と、

前記復号化アルゴリズム特定手段により特定された復号化アルゴリズムにより前記ファイル記憶手段に記憶されたファイルを復号してアクセスする処理手段と、

を備え、

身体情報により特定された復号化アルゴリズムにより復号可能なファイルのみをアクセス可能としたことを特徴とするコンピュータシステム。

【請求項2】複数の暗号化アルゴリズムを用いて暗号化された複数のファイルを記憶するファイル記憶手段と、前記ファイル記憶手段に記憶されたファイルと該ファイルのアクセスが認められている操作者の身体情報とを対応付けて記憶するアクセス許可条件記憶手段と、

前記ファイル記憶手段に記憶されたファイルへのアクセスの要求を検出する検出手段と、

前記検出手段が前記要求を検出した際に、操作者の身体情報の入力を要求する手段と、

外部より入力された身体的情報に基づいて前記ファイル記憶手段に記憶されたファイルへのアクセスが認められているか否かを前記アクセス許可条件記憶手段を参照して判別するアクセス許可判別手段と、

前記アクセス許可判別手段がアクセスが許可されていると判別した際に、該ファイルを復号するアルゴリズムを実行するためのプログラムをロードし、該プログラムを実行することにより前記ファイルをアクセス可能とするアクセス手段と、

を備えることを特徴とするコンピュータシステム。

【請求項3】前記暗号化アルゴリズムは、データを暗号化すると共に圧縮するアルゴリズムであり、前記復号化アルゴリズムは、暗号化されたデータを復号化すると共に伸張するアルゴリズムからなる、

ことを特徴とする請求項1又は2に記載のコンピュータシステム。

【請求項4】前記操作者の身体情報を読み取る身体情報読取手段と前記身体情報読取手段による身体情報の入力を促すメッセージを表示する手段を含む、

ことを特徴とする請求項1、2又は3に記載のコンピュータシステム。

【請求項5】前記身体情報は、指紋データ、網膜パターンのデータ、音声パターンのデータ、顔画像のデータのいずれかから構成され、

前記身体情報読取手段は、指紋読取装置、網膜パターン読取装置、音声パターン読取装置、顔画像読取装置のい

ずれかから構成される、

ことを特徴とする請求項4に記載のコンピュータシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コンピュータのセキュリティ技術に関し、特に、指紋等の身体情報から各処理を実行する権限を有するか否かを判別するコンピュータシステムに関する。

【0002】

【従来の技術】コンピュータの機密保護のため、ユーザ（操作者）名及びパスワードをコンピュータに予め登録し、ログオン時等にユーザ名及びパスワードを入力させ、入力されたユーザ名及びパスワードがコンピュータシステムに登録されていない場合、ログオンを認めない方法が知られている。

【0003】

【発明が解決しようとする課題】しかし、ユーザ名及びパスワード等による機密保護では、他人が容易に推定出来ないようにパスワードを設定したり、パスワードを定期的に変更する等、ユーザに負担がかかる。また、システム管理者によりユーザID等が設定される場合には、ユーザIDを記憶、メモする等の負担がかかった。さらに、コンピュータシステムから要求がある度に、キーボード等からユーザ名、パスワード、ユーザID等を入力しなければならず、操作が煩雑であった。

【0004】また、セッション中の各所で、実行を許可するか否かをユーザIDによってチェックする方法では、与えられたユーザIDやパスワードをメモしたり、記憶する等の必要があり、セッション中にユーザが離席して他者が着席する可能性があるため、機密保護の万全を期し難かった。

【0005】この発明は上記実状に鑑みてなされたもので、ユーザに機密保護の負担をかけないコンピュータシステムを提供することを目的とする。

【0006】

【課題を解決するための手段】上記目的を達成するため、第1の発明に係るコンピュータシステムは、複数の暗号化アルゴリズムを用いて暗号化された複数のファイルを記憶するファイル記憶手段と、操作者の身体情報と復号化アルゴリズムを対応付けて記憶する特徴記憶手段と、外部より入力された操作者の身体情報に基づいて、前記特徴記憶手段を検索し、復号化アルゴリズムを特定する復号化アルゴリズム特定手段と、前記復号化アルゴリズム特定手段により特定された復号化アルゴリズムにより前記ファイル記憶手段に記憶されたファイルを復号してアクセスする処理手段と、を備え、身体情報により特定された復号化アルゴリズムにより復号可能なファイルのみをアクセス可能としたことを特徴とする。

【0007】上記目的を達成するため、第2の発明に係

るコンピュータシステムは、複数の暗号化アルゴリズムを用いて暗号化された複数のファイルを記憶するファイル記憶手段と、前記ファイル記憶手段に記憶されたファイルと該ファイルのアクセスが認められている操作者の身体情報とを対応付けて記憶するアクセス許可条件記憶手段と、前記ファイル記憶手段に記憶されたファイルへのアクセスの要求を検出する検出手段と、前記検出手段が前記要求を検出した際に、操作者の身体情報の入力を要求する手段と、外部より入力された身体的情報に基づいて前記ファイル記憶手段に記憶されたファイルへのアクセスが認められているか否かを前記アクセス許可条件記憶手段を参照して判別するアクセス許可判別手段と、前記アクセス許可判別手段がアクセスが許可されていると判別した際に、該ファイルを復号するアルゴリズムを実行するためのプログラムをロードし、該プログラムを実行することにより前記ファイルをアクセス可能とするアクセス手段と、を備えることを特徴とする。

【0008】これらの構成によれば、操作者の身体情報に基づいて復号化アルゴリズムが特定される。従って、各操作者は、この復号化アルゴリズムを用いて復号できるファイルのみをアクセスでき、他のファイルをアクセスすることはできない。従って、正当権限を有する者のみが各ファイルをアクセスできる。また、ユーザ名、パスワード等をいちいち入力する必要がなく、操作性も高い。

【0009】前記暗号化アルゴリズムは、データを暗号化すると共に圧縮するアルゴリズムであり、前記復号化アルゴリズムは、暗号化されたデータを復号化すると共に伸張するアルゴリズムからなる、ことが望ましい。このような構成とすれば、限られた容量のファイル記憶手段を有効に使用することができる。

【0010】前記操作者の身体情報を読み取る身体情報読取手段と前記身体情報読取手段による身体情報の入力を促すメッセージを表示する手段を設けても良い。

【0011】前記身体情報は、指紋データ、網膜パターンのデータ、音声パターンのデータ、顔画像のデータ等からなる。この場合、前記身体情報読取手段は、指紋読取装置、網膜パターン読取装置、音声パターン読取装置、顔画像読取装置等から構成される。

【0012】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して説明する。

（第1の実施の形態）図1～図4を参照して、この発明の第1の実施の形態に係るコンピュータシステムを説明する。

【0013】図1に示すように、このコンピュータシステムは、指紋読取装置1と、キーボード2と、表示装置3と、外部記憶装置4と、メモリ5と、制御部6と、これらを接続するバスBから構成されている。

【0014】指紋読取装置1は、人間の指紋の画像を読

み取って、その画像データをRS232Cインタフェース等を介してコンピュータ本体1に供給する。

【0015】キーボード2は、文字、記号、数字等のデータを入力するための入力装置である。表示装置3は、CRT、液晶ディスプレイ等から構成され、キーボード2から入力されたデータ、操作者へのメッセージ等を表示する。

【0016】外部記憶装置4は、ハードディスク装置等から構成され、制御部6が処理するファイル（プログラム、文書ファイル、画像ファイル、等を含む）を暗号化された状態で記憶する。例えば、このコンピュータシステムをA、B、Cの3人で使用する場合には、図2に示すように、Aのアクセスするファイルは暗号化アルゴリズムHaで暗号化され、Bのアクセスするファイルは暗号化アルゴリズムHbで暗号化され、Cのアクセスするファイルは暗号化アルゴリズムHcで暗号化されている。外部記憶装置4は、制御プログラム11とユーザマスタファイルを記憶する。ユーザマスタファイルは、A、B、Cの指紋データと、暗号化プログラムPHa～PHcと、復号化プログラムPHa⁻¹～PHc⁻¹を対応付けて記憶する。制御プログラム11は、暗号化及び復号化プログラムを制御する。制御プログラム11は、OS（オペレーティングシステム）の起動に続いて起動するように設定されている。

【0017】メモリ5は、RAM（Random Access Memory）等で構成され、制御部6の主メモリ及びワークエリア等として機能する。制御部6は、MPU（Micro Processing Unit）等で構成され、主メモリに格納されたプログラムを実行し、指紋読取装置1、表示装置3、外部記憶装置4に対して、それぞれ指紋読み取り、画像表示、データの書き込みもしくは読み込みを指示する。また、制御部6は、指紋読取装置1によって読み取られた指紋の画像データの処理、キーボード2から入力された文字等のデータの処理、表示装置3に表示する画面データの処理、外部記憶装置4からのデータの読み込み処理、外部記憶装置4へのデータの書き込み等処理を行う。

【0018】次に、この実施の形態のコンピュータシステムの動作を図3のフローチャートを参照して説明する。このコンピュータシステムが起動されると、まず、OSを起動し（S11）、続いて、制御プログラム11を起動する（S12）。

【0019】次に、制御プログラム11は、指紋を入力すべき旨のメッセージを表示装置3に表示する（S13）。さらに、指紋読取装置1に指紋の読み取りを指示する（S14）。操作者はこの表示に従って指紋読取装置1から指紋を入力する（S15）。指紋読取装置1は、読み取った画像データ（指紋の画像データ）をインタフェースを介してメモリ5に格納する。制御プログラム11は、メモリ5に格納された指紋の画像データをコ

ード化し、コード化指紋データを生成する(S16)。次に、コード化指紋データとユーザマスタファイルの指紋データを照合し(S17)、一致するものがあるか否かを判別する(S18)。

【0020】一致するものがある場合には、その操作者がこのコンピュータシステムを使用することが認められていると判断し、図4に示すように、主メモリ(メモリ5)に制御プログラム11と対応する暗号化・復号化プログラムを常駐させる(S19)。以後は、データ読み出す時は、復号化プログラムを用いて暗号化されているプログラム・データ等を復号化して、読み出し、データ書き込む時は、暗号化プログラムを用いて暗号化してプログラム・データ等を書き込みながら、プログラムを実行する。

【0021】一方、指紋読取装置1から読み取った指紋の画像データがユーザマスタファイルに登録されている指紋データのいずれとも一致しないと判断した場合(S18)、制御プログラム11は、その操作者がこのコンピュータシステムを使用することが認められていないと判断し、主メモリへの制御プログラム11の常駐を中止する(S20)。以後は、通常の動作に移行する。

【0022】このような構成によれば、コンピュータの使用が認められている者の利用時は、制御プログラム11と共に操作者に対応する暗号化・復号化プログラムが主メモリに常駐する。従って、図2に示すように、外部記憶装置4に格納されている各種データを復号化プログラムで復号して通常のプログラム又はデータとして読み出して、処理することができる。また、作成・加工したデータを、制御プログラム11の制御下に暗号化プログラムを用いて暗号化して外部記憶装置4に格納することができる。

【0023】しかも、コード化指紋データで特定される操作者に対応する暗号化・復号化プログラムのみが主メモリに常駐する。従って、各操作者は、他の操作者用の暗号化アルゴリズムで暗号化されたファイルをアクセスすることができない。従って、各ファイルへのアクセスを正当権限を有する者に限定することができる。一方、操作者が非登録者の場合には、制御プログラム11が主メモリに常駐しない。従って、外部記憶装置4に格納されているプログラム及び各種データを復元することができない。従って、このシステム自体を使用すること自体が困難となる。

【0024】例えば、操作者Aがこのコンピュータシステムを使用する場合には、AはステップS15で指紋を入力し、ステップS16でこの指紋の画像データがコード化され、ステップS18でAの指紋の画像データから生成されたコード化指紋データとユーザマスタファイルのAの指紋データが一致すると判別される。主メモリには、制御プログラム11と共にA用の暗号化プログラムPHaとその復号化プログラムPHa⁻¹が常駐する(S

19)。

【0025】従って、操作者Aは、暗号化プログラムPHaを用いて暗号化されているプログラム1、2、文書ファイル1~3、画像ファイル等を復号化プログラムPHa⁻¹で復号化しながらアクセスし、さらに、作成及び加工した文書や画像を暗号化して外部記憶装置4に格納することができる。

【0026】ここで、Aが、例えば、Bがアクセス権を有するファイルをアクセスしようとしても、Bのファイルは暗号化プログラムPHbにより暗号化されているので、主メモリに常駐している復号化プログラムPHa⁻¹では、これを復号化できない。従って、Aは、Bのファイルをアクセスできない。従って、外部記憶装置4を共用しつつも、他者に秘密状態でファイルを使用できる。

【0027】(第2の実施の形態)第1の実施の形態においては、ログイン時の個人認証に指紋データを使用した。例えば、ファイルのアクセスが要求される度に操作者を認証することも可能である。このような処理を行う第2の実施の形態を以下に説明する。

【0028】この実施の形態のコンピュータシステムの物理的構成は基本的に図1に示す構成と同一である。一方、この実施の形態のコンピュータシステムは、論理的には、図5に示すように、OS(オペレーティングシステム)21と、ファイル制御プログラム31とから構成されている。

【0029】OS(オペレーティングシステム)21は、キーボード2の入力操作を検出する入力部22と、入力部22により検出された入力指示に従った処理を実行する処理部24と、表示装置3を制御する表示制御部23を備える。処理部24は、ファイルをアクセスするためのファイル処理部25を含む。

【0030】一方、ファイル制御プログラム31は、イベントが発生したことを検出し、そのイベントがファイル操作に関するものである場合に、そのファイル操作を許可するか拒否するかを制御するためのプログラムである。

【0031】図5は、OS21が、DOS(ディスクオペレーティングシステム)であるとした場合の例であり、ファイル制御プログラム31は、入力フック部32と、ドライバ部33と、ユーザマスタファイル39とから構成される。

【0032】入力フック部32は、割り込み要求が発行されたとき(イベントが発生したとき)、ファイル制御プログラム31が存在しないときに行われるべき処理を行わず、該処理に先立ちドライバ部33に処理を行わせる(フックする)。

【0033】ユーザマスタファイル39は、図6に示すように、ユーザ毎、即ち、指紋データ毎に操作できるファイルのリストからなる。なお、このユーザマスタファイル39自体は、このコンピュータシステムの管理者の

みがアクセスできるように設定されている。ドライバ部33は、処理内容判別部34と、メッセージ表示部35と、コード化部36と、判別部37と、送信部38とから構成される。

【0034】処理内容判別部34は、入力フック部32により取り込まれた入力情報を解析し、その内容がファイルの操作を指示しているか否かを判別し、指示している場合には、コード化部36に指紋の読み取りを指示すると共に判別部37に入力情報を提供する。また、フックされた入力情報がファイルの操作を指示していない場合には、検出信号を送信部38に送る。

【0035】メッセージ表示部35は、処理内容判別部34が「入力ファイルの操作を指示している」と判別した場合に、指紋情報の入力を促す画面をOS21の表示制御部23を介して表示装置3に表示する。また、判別部37が「要求されたファイル操作がその操作者に認められていない」と判断した際に、アクセスが拒否されたことを示す画面を表示制御部23を介して表示装置3に表示する。

【0036】コード化部36は、処理内容判別部34からの指示に従って指紋読取装置1に指紋の読み取りを指示し、また、指紋読取装置1から指紋の画像を取り込み、これをコード化し、コード化指紋データを生成する。

【0037】判別部37は、コード化部36で生成されたコード化指紋データに基づいて、ユーザマスタファイル39を参照し、そのコード化指紋データを有する者が該当ファイルをアクセスする権限を有するか否かを判別する。そして、権限を有すると判断した場合には、送信部38にアクセスを許可する信号を送信する。また、権限を有していないと判別した場合には、メッセージ表示部35にアクセスを許可しない旨のメッセージを表示させる。

【0038】第2の実施の形態のコンピュータシステムの動作を図7及び図8のフローチャートを参照して説明する。まず、コンピュータの電源が投入されると、OS21が起動する(S31)。次に、ファイル制御プログラム31が起動する(S32)。ファイル制御プログラム31の入力フック部32は、起動すると、OS21の入力部22が発生する割り込み要求に対応する処理のアドレスを、処理部24からドライバ部33のアドレスに書き換える。換言すると、入力部22が発生するキー操作の検出信号等の送信先を入力フック部32のアドレスに書き換える(S33)。

【0039】例えば、OS21がマイクロソフト社から提供されているMS-DOS(登録商標)の場合には、主メモリとして機能するメモリ5上に作成される割り込みテーブル中、入力に関するシステムコールの割込INT21に対応する処理のアドレスをドライバ部33のアドレスとする。以上で、起動時の設定動作は終了する。

【0040】この状態で、キーボード2から何らかの入力があると、OS21の入力部22は、この入力操作を判別し、必要に応じて割り込み要求を発する(IOイベントの発生)。この割り込み要求に対応する処理は、通常は処理部24で行うが、ファイル制御プログラム31の起動時にドライバ部33のアドレスに書き換えられている。従って、処理はドライバ部33に移行され、フックされる(図8、S41)。

【0041】処理内容判別部34は、OS21から入力された検出信号を解析し(S42)、入力内容がファイルの操作(ファイルを開く、実行ファイルを起動する等)を指示しているか否かを判別する(S43)。入力内容がファイルの操作を指示している場合には、コード化部36を介して指紋読取装置1に指紋の読み取りを指示する(S44)。さらに、メッセージ表示部35に指紋の入力を促すメッセージの表示を指示する(S45)。メッセージ表示部35は、処理内容判別部34の指示に従い、OS21の表示制御部23を介して表示装置3に、指紋の入力を促すメッセージを表示する。

【0042】コード化部36は、指紋読取装置1からの指紋の画像データの入力を待機し(S46)、画像データが入力されると、この画像データをコード化指紋データに変換し、判別部37に提供する(S47)。判別部37は、ユーザマスタファイル39を参照し、コード化部から供給されたコード化指紋データを有する者が、入力操作で指示されたファイルの操作を認められているか否かを判別する(S48)。

【0043】判別部37は、アクセスが認められていると判断すると、主メモリにそのファイルをアクセスするために必要な暗号化プログラムと復号化プログラムを常駐させる(S49)。続いて、判別部37は、送信部38に検出信号を供給する。送信部38は処理をOS21の処理部24に引き渡す(S50)。

【0044】以後、処理部24は、復号化プログラムにより指示されたファイルを復号化して読み出し、加工・生成したデータを暗号化プログラムにより暗号化して書き込む。そのファイルのアクセスが完了すると、ファイル制御プログラム31は、主メモリ上の圧縮プログラム及び復号化プログラムを削除する。

【0045】一方、ステップS48で、判別部37によりファイル操作が認められていないと判断された場合、メッセージ表示部35は、OS21の表示制御部23を介して表示装置3に「アクセスが許可されていません」等のファイル操作を拒否するメッセージを表示する(S51)。ステップS43で、処理内容判別部34が、指示内容がファイルの操作ではないと判断した場合には、送信部38によりOS21の処理部24に処理が引き渡される(S52)。処理部24は、この指示に対応する処理を行う。

【0046】また、システムをシャットダウンする際に

は、OS 21の入力部22が発生する割り込み要求に対応する処理のアドレスを通常のアドレスに書き換えてから終了する。このような構成によれば、例えば、デスクトップ上で任意のプログラムの起動を指示した場合には、この指示が入力フック部32でフックされ、判別部37でアクセスを許可するか否かがユーザマスタファイル39に従って判別され、許可の場合のみ、対応する暗号化・復号化プログラムが起動され、そのファイルをアクセスすることができる。

【0047】以上説明したように、この第2の実施の形態によれば、ファイル制御プログラム31が、入力指示を自動的に取り込んで、指示されたファイルをアクセスする権限を有するか否かをコード化指紋データに基づいて判別し、権限を有する場合にはそのファイルのアクセスを許可する。従って、ユーザに負担をかけることなくコンピュータの機密保持を実行することができる。

【0048】また、ファイル制御プログラム31をインストールするだけでファイル操作を制御することができ、既存のOS、アプリケーションプログラム等に修正を加える必要がなく、そのまま使用することができる。

【0049】なお、以上の説明では、起動時にファイル制御プログラム31が、入力部22の割り込み要求に対応する処理のアドレスを書き換え、ファイル制御プログラム31のインストール時に、割り込み要求に対応する処理のアドレスを書き換え、アンインストール時に元のアドレスに書き換えてもよい。

【0050】暗号化アルゴリズム及びそれを実現するプログラムは、データを暗号化すると共に圧縮するものが望ましく、前記復号化アルゴリズム及びそれを実現するプログラムは、暗号化されたデータを復号化すると共に伸張するものが望ましい。このような構成によれば、外部記憶装置4の記憶容量を有効に利用することができる。

【0051】OS 21は、DOSに限定されず、いわゆる、ウィンドウシステム、unix等、任意のものを使用することができる。これらのOSを使用する場合には、各OSのプロパティに応じて、適宜ファイルへのアクセス或いは割り込みの要求、リンクの発生等の所定のイベントを検出し、指紋データの入力を促すと共に操作者がファイルをアクセスする権限を有するか否かを判別すればよい。

【0052】なお、指紋読取装置1とコンピュータ本体とはネットワーク等で接続されてもよい。

【0053】以上の実施の形態では、個人認証のために、コード化指紋データを使用した、指紋データの種類の任意である。例えば、指紋の画像データをフーリエ変換し、その位相情報を抽出し、これを指紋データとして使用することも可能である。この場合は、例えば、予め登録しておいた位相情報と指紋読取装置で読み取った画像から抽出した位相情報の相関度を比較し、相関度

が一定レベル以上の場合に、2つの指紋が一致すると判断する。

【0054】以上の実施の形態では、個人認証のために、指紋を使用した、網膜の血管パターン、音声パターン、顔の画像等を認証情報として使用することも可能である。

【0055】なお、この発明のコンピュータは、専用のシステムによらず、通常の指紋読取装置等と通常のコンピュータシステムを用いて実現可能である。例えば、指紋読取装置を接続したコンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、CD-ROM等）から該プログラムをインストールすることにより、上述の処理を実行するコンピュータシステムを構成することができる。

【0056】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的且つ流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（BBS）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、OSの制御下に、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【0057】

【発明の効果】以上説明したように、この発明によれば、ユーザの身体情報に基づいて、ユーザにほとんど負担をかけることなく、機密を保持することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態によるコンピュータシステムの物理的構成を示すブロック図である。

【図2】外部記憶装置の構成を示す概念図である。

【図3】図1の制御部において実行される起動時の制御処理を示すフローチャートである。

【図4】暗号化・復号化プログラムによるデータ処理の様子を示す図である。

【図5】本発明の第2の実施の形態によるコンピュータシステムの物理的構成を示すブロック図である。

【図6】ユーザマスタファイルの例を示した図である。

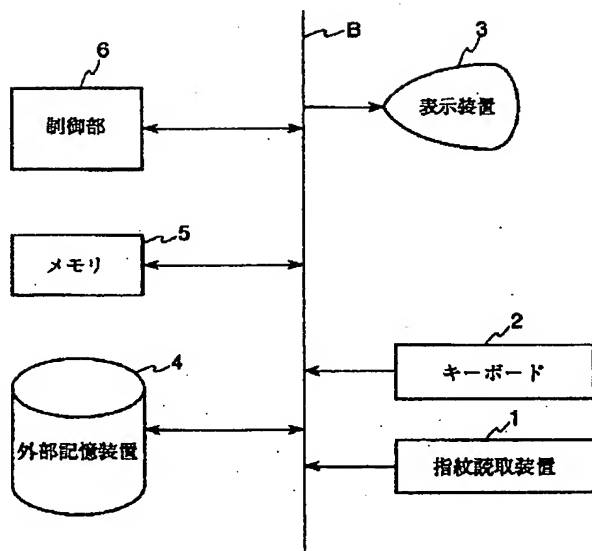
【図7】第2の実施の形態のコンピュータシステムの起動時の処理を示すフローチャートである。

【図8】第2の実施の形態のコンピュータシステムの入力操作時の処理を示すフローチャートである。

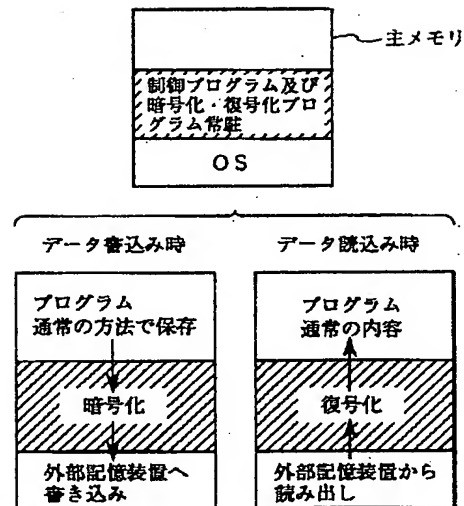
【符号の説明】

- 1 指紋読取装置
- 2 キーボード
- 3 表示装置
- 4 外部記憶装置
- 5 メモリ
- 6 制御部
- 11 制御プログラム

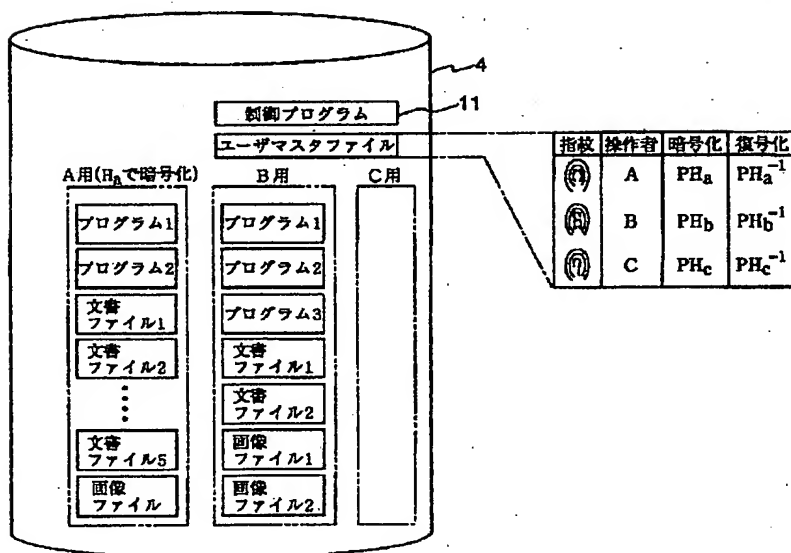
【図1】



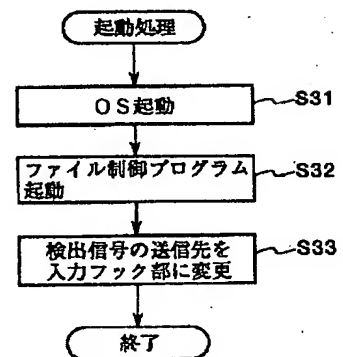
【図4】



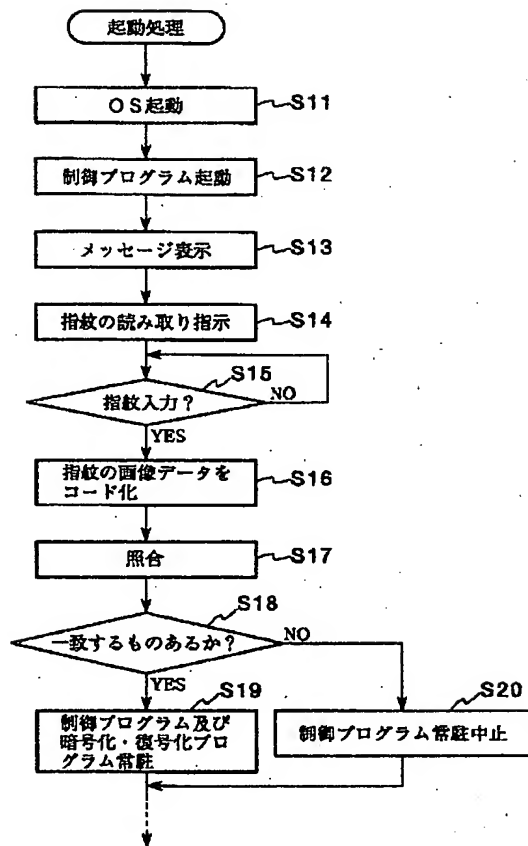
【図2】



【図7】



【図3】

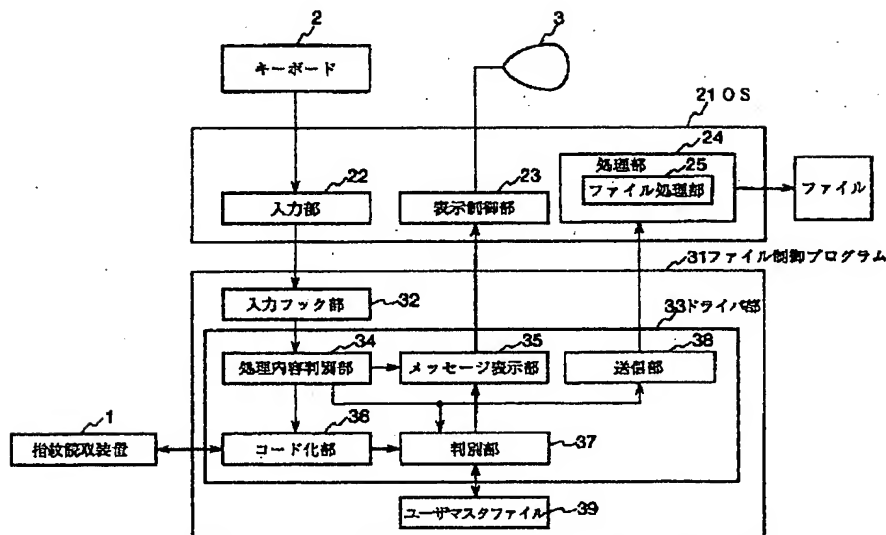


【図6】

	ファイル1	ファイル2	ファイル3	ユーザマスタファイル
A	○	○	×	×
B	×	○	○	×
...
Z	○	○	○	○

Z: システム管理者

【図5】



【図8】

